PCT/DE 03/00805

BUNDESREPUBLIK DEUTSCHLAND

10/507426

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 11 674.1

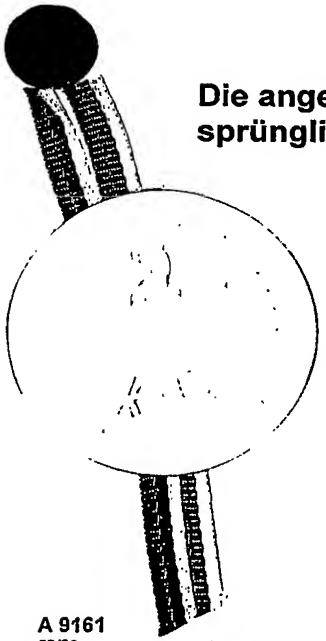
Anmeldetag: 15. März 2002

Anmelder/Inhaber: T-Mobile Deutschland GmbH, Bonn/DE

Bezeichnung: Verfahren zur Bereitstellung und Abrechnung von WIM-Funktionalitäten bei mobilen Kommunikations-sendeeinrichtungen

IPC: H 04 M, H 04 Q

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.



München, den 8. April 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

A 9161
03/00
EDV-L

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH

15.03.2002

T-Mobile Deutschland GmbH

Verfahren zur Bereitstellung und Abrechnung von WIM-Funktionalitäten bei mobilen Kommunikationsendeinrichtungen

Die Erfindung betrifft ein Verfahren zur Bereitstellung und Abrechnung von WIM-Funktionalitäten bei mobilen Kommunikationsendeinrichtungen.

Stand der Technik

Für gesicherte elektronische Geschäfte über Mobilfunk wurde / wird unter anderem von den Mobilfunknetzbetreibern und Geräteherstellern gemeinsam ein als WTLS (Wireless Transport Layer Security) bezeichneter offener Standard entwickelt. WTLS basiert auf bestehenden Normen, wie WAP (Wireless Application Protocol) und TLS (Transport Layer Security), zur Verschlüsselung und einem WIM (Wireless Identification Module) zur Identifizierung und Signatur. Bei der TLS bzw. WTLS Technologie handelt es sich um ein Protokoll der Transportschicht. Diese Schicht gewährleistet von Haus aus eine zuverlässige, transparente und verschlüsselte Datenübertragung zwischen zwei Systemen basierend auf einem sogenannten Public Key Verschlüsselungsverfahren (PKI). Zudem fungiert sie als Schnittstelle zwischen den darüber liegenden anwendungsorientierten Schichten und den darunter liegenden netzwerkorientierten Schichten. Die zentrale Aufgabe ist der Verbindungsaufbau und die Steuerung zwischen zwei Prozessen. Die Identifizierung und Signatur der Informationen erfolgt mittels der WIM.
Signaturen, die während des Handshake im WLTS/TLS erfolgen sind nicht benutzerinitiiert und geschehen automatisch. Hierzu wird auch ein eigener Schlüssel (Key) verwendet, der nicht der Signaturkey ist, der für Signaturen innerhalb von Applikationen verwendet wird.

Dies erlaubt es, mit mobilen Kommunikationsendgeräten verschiedenste Transaktionen durchzuführen, wie z. B. Bank- und Börsengeschäfte, Kreditkarten- und andere Zahlungen sowie Zugangskontrolle zu Gebäuden sowie Computern. Zusammen mit geeigneten Infrarotschnittstellen oder dem Kurzstreckenfunk „Bluetooth" sind Zahlungen in Verbindung mit Kassen und Zapfsäulen sowie Autorisierungen bei Schließsystemen denkbar.

Die notwendigen PKI Verfahren werden individuell zwischen einem Teilnehmer (Kunden) und einem beliebigen Dienstleister durchgeführt, wobei sich der Teilnehmer beim Dienstleister entsprechend registriert. Die WIM dagegen wird in der Regel vom Betreiber des vom Endgerät verwendeten Kommunikationsnetzes bereitgestellt und ist in einem Endgerät oder einem mit diesem verbundenen Identifikationsmodul, z. B. SIM, realisiert.

Gegenstand der Erfindung

Die Aufgabe der Erfindung besteht darin, ein Verfahren vorzuschlagen, das ein einfaches und sicheres Bereitstellen und Abrechnen von WIM-Funktionalitäten bei mobilen Kommunikationsendgeräten erlaubt.

Diese Aufgabe wird erfindungsgemäß durch die Merkmale des Patentanspruchs 1 gelöst.

Vorteilhafte Ausgestaltungen und Weiterbildungen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Es wird vorgeschlagen, die Anzahl der Signaturen, die ein Kommunikationsendgerät bzw. ein Identifikationsmodul, z. B. eine SIM Chipkarte, durchführen kann, durch einen Zähler zu begrenzen. Mit jeder Signatur wird der Zähler weitergezählt. Wenn der Zähler einen Schwellwert erreicht hat, ist keine weitere Signatur möglich, bevor nicht durch eine Art Freischaltung / Aufladung ein Reset auf den Zähler stattgefunden hat.

Erfindungsgemäß stellt die WIM eine Funktion zur Verfügung, mit der auf Applikationsebene Signaturen erstellt werden können. Diese sind durch den Teilnehmer (Benutzer) initiiert; der Teilnehmer muss z.B. für jede Signatur seine sogenannte PIN-NR (non repudiation PIN) eingeben.

Die WIM sperrt die Funktionalität „Signieren" wenn ein Zähler abgelaufen ist. Eine Freischaltung / Aufladung kann dann z. B. per ÖTA (over the air message) erfolgen und gegenüber dem Teilnehmer entsprechend vergebührt werden.

Nachfolgend wir ein Ausführungsbeispiel der Erfindung beschrieben. Als mobile Kommunikationsendeinrichtung wird von einem Mobiltelefon mit Identifikationsmodul (SIM-Karte) ausgegangen, das über Einrichtungen zur Durchführung gesicherter elektronischer Geschäfte und entsprechende Schnittstellen verfügt.

Die WIM zählt intern jede durch den Teilnehmer initiierte Signatur. Wenn eine voreingestellte Anzahl von Signaturen geleistet wurde, sind keine weiteren Signaturen möglich, bevor nicht diese Funktion wieder freigeschaltet wird. Die Freischaltung geschieht über die Luftschnittstelle des Mobilkommunikationsnetzes (over the air) mit Hilfe einer entsprechenden, auf der SIM-Karte implementierten SAT-Applikation (SAT: SIM Application Toolkit) und kann nur durch den Netzbetreiber erfolgen. Gleichzeitig mit der Freischaltung kann die Anzahl der möglichen Signaturen neu gesetzt werden. Eine Zählung jeder einzelnen Signatur im Mobilkommunikationsnetz ist nicht erforderlich.

Vielfältige Möglichkeiten sind denkbar und können kombiniert werden:

- Die Signatur kann generell freigeschaltet werden, z. B. für Postpaid-Teilnehmer, d.h. Teilnehmer mit SIM-Kartenvertrag oder Teilnehmer, die eine höhere Grundgebühr bezahlen.
- Der Zählerstand auf der Karte kann vom Teilnehmer lokal durch eine einfache SAT-Funktion abgefragt werden, z. B. um rechtzeitig die Freischaltung weiterer Signaturen, z. B. über eine SAT-Funktion, zu beantragen. Die Freischaltung wird vergebührt.

- Die Karte sendet nach dem Verbrauchen der letzten Signatur eine SMS an eine an das Kommunikationsnetz angebundene zentrale Einrichtung, z.B. einen Freischalteserver, der den Teilnehmer mit der Anzahl der verbrauchten Signaturen vergebührt und anschließend die Signaturfunktion wieder freigibt, sofern der Teilnehmer die Freigabe wünscht (für Prepaid und Postpaid anwendbar).

Der interner Zähler wird bei jeder Signatur heruntergezählt. Die WIM Funktion wird gesperrt, wenn der Zählerstand = 0 erreicht ist. Eine Freischaltung erfolgt „over the air" z. B. durch eine SAT-Anwendung. Ein unbegrenztes Signieren kann z.B. durch Setzen des Zählerstands auf einen Wert von -1 durch den Netzbetreiber freigeschaltet werden.

Die Erfindung ermöglicht es Drittparteien, z. B. Banken, ihre eigenen PKI-Verfahren aufzubauen und ihre Teilnehmer selbst für die Nutzung dieser Verfahren zu registrieren. Der Netzbetreiber benötigt keine eigenen PKI-Verfahren, sondern stellt den Telnehmern lediglich eine universell nutzbare WIM zur Verfügung.

Patentansprüche

1. Verfahren zur Bereitstellung und Abrechnung von WIM-Funktionalitäten bei mobilen Kommunikationsendeinrichtungen,
dadurch gekennzeichnet,
dass die WIM intern jede durch den Teilnehmer initiierte Signatur zählt, wobei die Signaturfunktion gesperrt wird, wenn eine vorgegebene Anzahl von Signaturen geleistet wurde.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass durch die Freischaltung / Aufladung der Zähler auf einen vorgegebenen Wert gesetzt wird, und dadurch die Signaturfunktion erneut für eine vorgegebene Anzahl von Signaturen freigegeben wird.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass bei jeder Freischaltung / Aufladung eine Gebührenabrechnung der durchgeführten Signaturen gegenüber dem Teilnehmer erfolgt.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Freischaltung / Aufladung der Signaturfunktion über die Luftschnittstelle des mobilen Kommunikationsnetzes erfolgt.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Freischaltung / Aufladung durch einen an das mobile Kommunikationsnetz angebundenen Freischalteserver erfolgt.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Bereitstellung und Abrechnung von WIM-Funktionalitäten bei mobilen Kommunikationsendeinrichtungen, das sich dadurch auszeichnet, dass die WIM intern jede durch den Teilnehmer initiierte Signatur zählt, wobei die Signaturfunktion gesperrt wird, wenn eine vorgegebene Anzahl von Signaturen geleistet wurde. Es ist keine weitere Signatur möglich, bevor nicht durch eine Art Freischaltung / Aufladung ein Reset auf den Zähler und eine entsprechende Vergebührung stattgefunden hat.